

WiFi captive portal bypass

Get out of jail free the time of a lightning talk

Cédric BLANCHER

cedric.blancher@eads.net
EADS Corporate Research Center
EADS/CCR/DCR/SSI

sid@rstack.org
Rstack Team
<http://sid.rstack.org/>

Eusecwest/core06 - London - UK
2006 February 20-21
<http://eusecwest.com/>



Authorization tracking

Captive portal system has to identify authenticated users connections

- MAC address
- IP address
- MAC and IP addresses

Idea : find someone authenticated and spoof his box

Can we spoof thoses parameters ?

MAC or IP based authorization tracking

Single network parameter spoofing is no pain to deal with

- MAC address spoofing

```
joker# ifconfig ath0 hw ether $MAC
```

Just use a unique IP and everything's fine

- IP spoofing is achieved through ARP cache poisoning based MiM

See refs[BLA02][ARPS][MISC] for details

MAC and IP tracking bypass

Two steps packets mangling

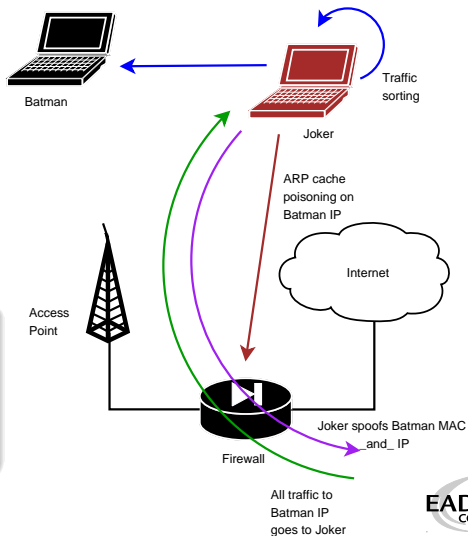
- 1 ARP cache poisoning MiM based IP spoofing
- 2 Replace source MAC address before sending

We could put hundreds C code lines to do that

Lazy guys will use Linux stock 2.6 kernel features :)

- Iptables[IPT]
- Ebtables[EBT]

See refs[BLA05] for details



Demo

We Proudly R3wt



Thank you for your attention and...

Greetings to

- EADS CCR/DCR/STI/C team
- **Rstack.org** team
<http://www.rstack.org/>
- **MISC Magazine**
<http://www.miscmag.com/>
- **French HoneyNet Project**
<http://www.frenchhoneynet.org/>



Download these slides from <http://sid.rstack.org/>

Shameless plug

Planing to attend Cansecwest/core06 in Vancouver?
Interested in fooling/pentesting/protecting your wireless network?



You may want to attend
Practical WiFi (in)Security Masters Security Dojo

See <http://cansecwest.com/dojowifi.html>

References



[ARPS] Arp-sk, <http://sid.rstack.org/arp-sk/>



[BLA02] C. Blancher, Switched environments security, a fairy tale, 2002,
http://sid.rstack.org/pres/0207_LSM02_ARP.pdf



[BLA05] C. Blancher, Attacking WiFi networks with traffic injection, 2005,
http://sid.rstack.org/pres/0511_Pacsec_WirelessInjection



[EBT] Ebttables, <http://ebtables.sourceforge.net/>



[IPT] Iptables, <http://www.netfilter.org/>



[MISC] MISC Magazine, <http://www.miscmag.com/>

